SERVER EDITION
FOR MS WINDOWS

User Manual – Version 5

September 2009
Version 1.1

Table of contents

1 INTRODUCTION 3
1.1 OVERVIEW 3
1.2 SYSTEM REQUIREMENTS 4
2 INSTALLATION 5
2.1 MSI INSTALL OPTIONS 5
2.2 THE SETUP WIZARD 6
2.3 SECURITY – ACCESS TO THE BACKUP CLIENT 9
2.4 SERVER EDITION AUTO-UPDATE 9
3 THE BACKUP SERVICE 10
3.1 SERVER EDITION RUNNER 10
4 BACKUP CLIENT 11
4.1 HOW TO BACKUP 12
4.2 HOW TO RESTORE 14
4.3 OPTIONS AND SETTINGS 16
4.4 ADDITIONAL SETTINGS 22
5 PLUG-INS 27
5.1 EMAIL NOTIFICATION 28
5.2 SYSTEM STATE PLUG-IN 29
6 SECURITY 30
7 SWISSVAULT SUPPORT 31

1 Introduction

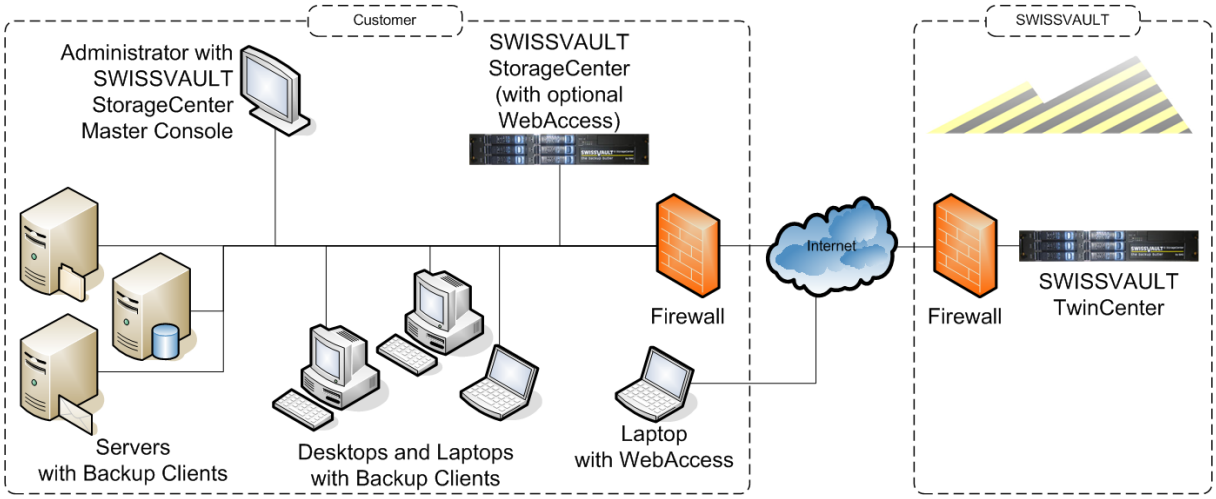
Congratulations on choosing SWISSVAULT. We believe you will find SWISSVAULT to be the most secure, scalable and efficient solution in addressing the business risk associated with the protection of critical data in a distributed environment. If you experience any difficulty during the installation of SWISSVAULT, please contact your software provider.

SWISSVAULT Server Edition (SE) is a remote storage solution that utilises client/server architecture to securely replicate data from the client device to a central data server. Data is compressed to minimise bandwidth utilisation and transferred using a secure SSL connection to the server. The data is stored in an encrypted format, using an encryption key known only to you.

SWISSVAULT minimises risk, maximises productivity and allows businesses to regain control of their most valuable asset – their data.

1.1 Overview

SWISSVAULT Server Edition manages the backup and retrieval of files and/or folders on your server. Selected files are backed up to the StorageCenter that is installed on a remote server. This is shown in the following diagram:



Your Backup Client connects to a group on the StorageCenter during the installation. The Group Administrator oversees all group members, using the Backup Monitor. The StorageCenter administrator uses the StorageCenter Console to manage the entire StorageCenter, including all the different groups.

1.2 System Requirements

Operating System

- Microsoft Windows Server 2003 (incl. SBS bundles)
- Microsoft Windows Server 2000 (incl. SBS bundles)

Processor & Memory

Required: Pentium III processor with 256MB memory above operating requirements
Recommended: Processor and memory requirements increase with the amount of data protected by Server Edition:

Amount of data Protected	Recommended Processor	Recommended Memory
Less than 100GB	Pentium III 500MHz	512MB
200GB	P4 entry level	512MB
500GB	P4 2.0GHz	1GB
1TB	Dual Xeon 3GHz	2GB

Disk Space

- Required: 50 MB plus space for local cache.
- Recommended: Amount of free space equal to the backup account limit if Binary Patching is enabled. The space requirement for Delta Blocking is considerably less. Please refer to the Patching section in Chapter 4 for more information.

File/Print Server: The local cache can be as large as the total size of all files selected for backup. A file selection of 10 GB needs up to 10 GB free space for the cache.

Database: Space is needed for the data dump, which can be as large as the database, as well space for the cache, which is compressed version of the database. Assuming 1:2 compression on a 10GB database you are recommended to have 15GB (10GB for the dump and 5GB for the cache) free space available. If the VSS plug-in is used, only the cache requirement is applicable.

Virtual Memory Recommendations

- Double the amount of RAM, with a minimum of 512MB (Total for all disk volumes)

Minimum Video Settings

- 800 x 600 Resolution, 256 colours

Other Hardware

- Network interface card or a virtual network adapter card
- CD-ROM drive or Internet access to download and install the software

Server Edition is also available for the following operating systems:

- Mac OS X Server (from version 10.4)
- Linux Red Hat v6 - v9 / Fedora

2 Installation

To install the SWISSVAULT Server Edition Client, simply run the installation file. The Backup Client requires working space for the cache and temporary disk space for creating patches. **Note: Please ensure that the drive where you install the Backup Client has enough free hard drive space to store a copy of the selected files.**

SWISSVAULT SE Setup
Welcome to the SWISSVAULT SE Setup Wizard
The Setup Wizard will install SWISSVAULT SE on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
SWISSVAULT
the backup butler
Back
Next
Cancel

For example, if you want to backup 10GB of data, there must be at least 10GB of free space available on the drive where you install the Backup Client. **Note: Plug-ins may also require additional working space. Please consult the applicable plug-in documentation.**
Options available during the installation process depend on what your administrator enabled when the MSI file was created, ranging from advanced install settings, including the JRE, to specifying the install location. The default install path is C:\Program Files\SWISSVAULT SE.

Click on **Next** to run through the available options and then **Install** to start the process. The Installer will extract the files and install the Backup Client.

When you open the Backup Client interface for the first time, the Setup Wizard will start automatically. You need to create an account for the Backup Client on the StorageCenter before you can initiate any backups.

2.1 MSI Install Options

The Backup Client MSI installer also enables you to remotely deploy the Backup Client using your preferred desktop management solution, e.g. Microsoft SMS. Use the Deployment Wizard and include the Name-Server and Group settings in the MSI; with these settings populated, you can specify that the Backup Account must be created automatically during the install process. Use the following command to run the installer:

./BackupClientFileName_SE.msi PREPACCOUNT=Yes

If you do not want to include the Name-Server and Group details you can also specify it as additional parameters, these will override the default settings configured:

- **SERVERIP** – The IP address of the Name-Server
- **GROUP** – Group Name
- **CREATEKEY** – Group Create Key

The standard MSI parameters are also available. A few examples are:

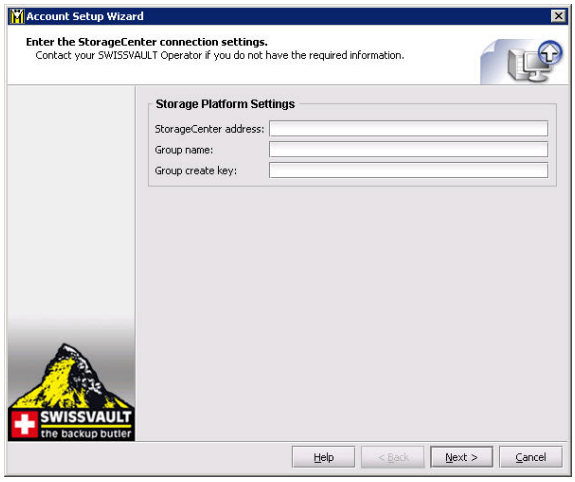
- /help – Help information
- /quiet – Quiet mode, no user interaction
- /passive – Unattended mode, progress bar only

MSI Notes:

1. SWISSVAULT will use the Windows Computer Name as the Backup account name.
2. The password and encryption keys are randomly selected during the account creation process.
3. You are advised to install a Group Certificate to the specific Groups as the encryption keys are random. Without this certificate you will not be able to connect to a backup account to restore any data, should the computer crash. The password can be changed in the StorageCenter Console.

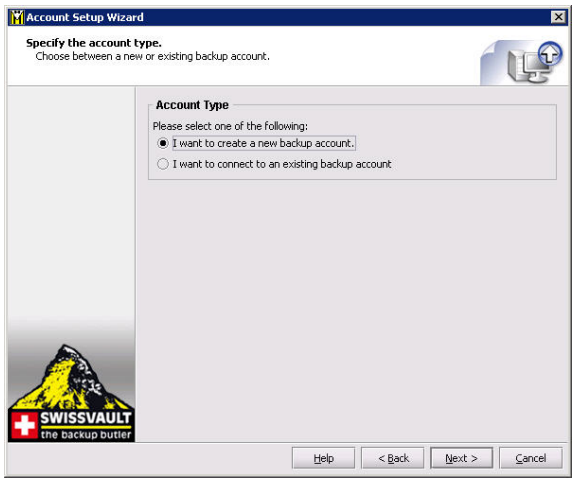
An example to deploy the Server Edition backup client:
...\SWISSVAULTSE5.0.msi **PREPACCOUNT**=YES **SERVERIP**=SERVERNAME **GROUP**=GROUP01 **CREATEKEY**=KEY021 /passive /quiet

2.2 The Setup Wizard



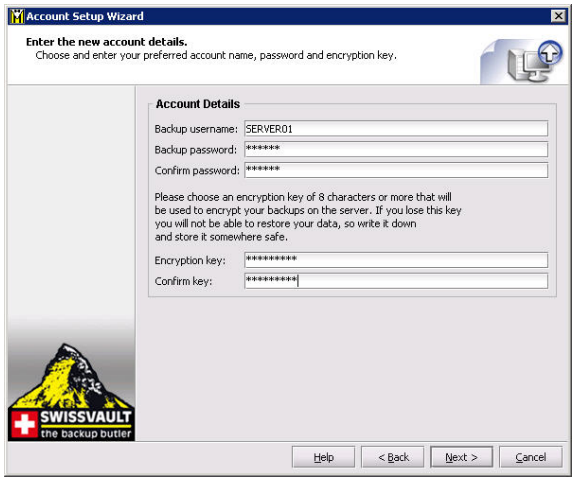
Step 1 of 8
Supply the correct Backup server and group settings. The StorageCenter address is the IP address or DNS name of the Name-Server that authenticates you before you can backup or restore data. The Group name specifies which group you will join and the Group create key is needed in order for the client to create an account in the specific group. Click **Next**.

Note: Ensure that you enter the correct settings. Contact your backup administrator if you are not sure about the settings.


Account Setup Wizard
Specify the account type.
Choose between a new or existing backup account.
Account Type
Please select one of the following:
I want to create a new backup account.
I want to connect to an existing backup account
Help
< Back
Next >
Cancel

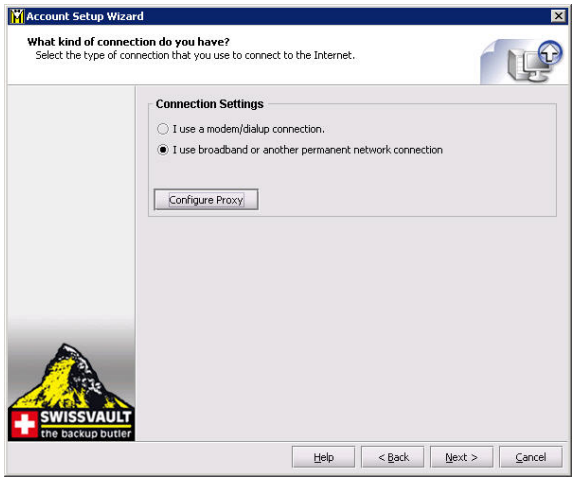
Step 2 of 8
If you are installing the backup software for the first time, select "**I want to create a new backup account**". If you have an existing account that you want to reconnect to, select the "**I want to connect to an existing backup account**" option. Click **Next** to continue.

Note: You cannot connect from different servers to the same backup account. Each server must have a separate account.


Account Setup Wizard
Enter the new account details.
Choose and enter your preferred account name, password and encryption key.
Account Details
Backup username: SERVER01
Backup password: ******
Confirm password: ******
Please choose an encryption key of 8 characters or more that will be used to encrypt your backups on the server. If you lose this key you will not be able to restore your data, so write it down and store it somewhere safe.
Encryption key: *********
Confirm key: *********
Help
< Back
Next >
Cancel

Step 3 of 8
Choose and enter your backup username, password and encryption key. The backup username and password can consist of any keyboard combination between 4 and 20 characters. The encryption key can be any keyboard combination between 8 and 55 characters. Click **Next**.

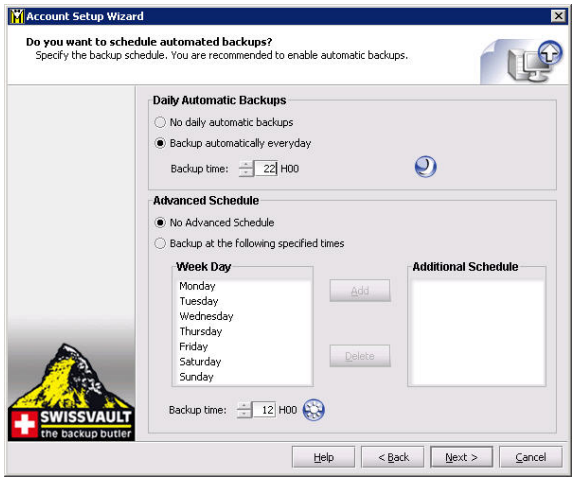
Do not forget your encryption key as you will not be able to retrieve your data without this information. We highly recommend storing two copies of the account details at two independent, safe locations.


Account Setup Wizard
What kind of connection do you have?
Select the type of connection that you use to connect to the Internet.
Connection Settings
I use a modem/dialup connection.
I use broadband or another permanent network connection
Configure Proxy
Help
< Back
Next >
Cancel

Step 4 of 8
Select the connection that you want to use to connect to the StorageCenter.

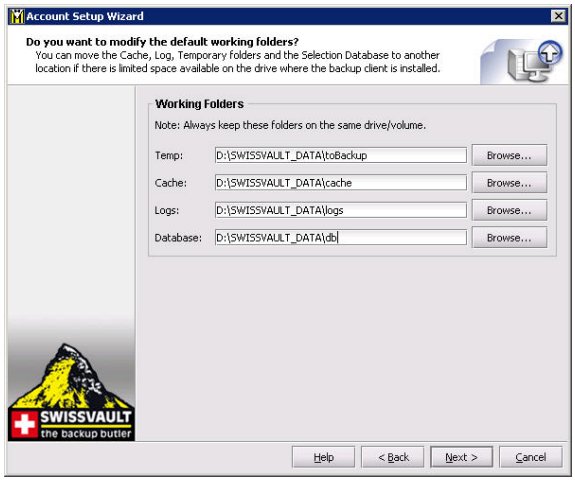
Use the **Configure Proxy** button to specify any Proxy settings needed for communications to the Internet. Click **Next** to continue.

If you select the modem/dialup connection, the next step will prompt you to supply the connection that you want to use.



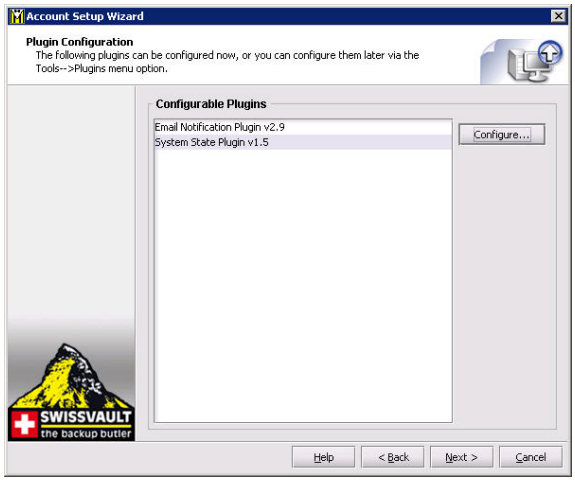
Step 5 of 8
In this step you can configure the daily and hourly automatic backup schedule. The default backup time is 19h00. It is advised to backup at night when the server is not in use. The server must be running at the time of scheduled backups, but you do not have to be logged in.

Note: If you do not schedule any backups, you will have to manually backup your data. We strongly recommend that you run automated backups.

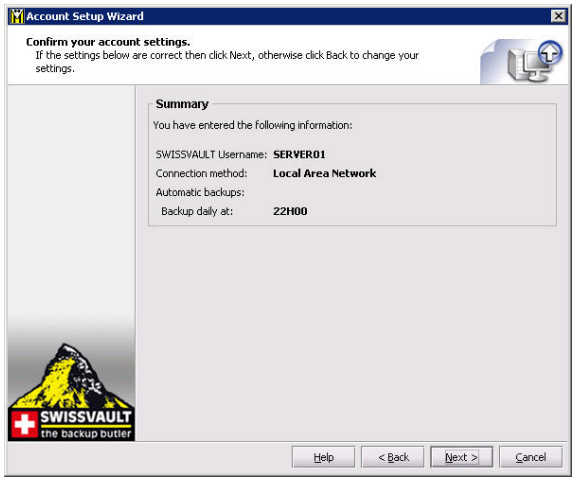

Account Setup Wizard
Do you want to modify the default working folders?
You can move the Cache, Log, Temporary folders and the Selection Database to another location if there is limited space available on the drive where the backup client is installed.
Working Folders
Note: Always keep these folders on the same drive/volume.
Temp:
D:\SWISSVAULT_DATA\toBackup
Cache:
D:\SWISSVAULT_DATA\cache
Logs:
D:\SWISSVAULT_DATA\logs
Database:
D:\SWISSVAULT_DATA\db
Browse...
Help
< Back
Next >
Cancel

Step 6 of 8
If you have limited space on the drive where the Backup Client is installed, you can move the Cache, Logs, Temporary folders and the selection database to another location.

Note: Always keep these folders and the selection database on the same drive/volume.


Account Setup Wizard
Plugin Configuration
The following plugins can be configured now, or you can configure them later via the Tools-->Plugins menu option.
Configurable Plugins
Email Notification Plugin v2.9
System State Plugin v1.5
Configure...
Help
< Back
Next >
Cancel

Step 7 of 8
You can select any of the available plug-ins in this step and click on **Configure** to enable and configure the plug-in(s). Alternatively, you can access and configure them later from the Tools menu. Note that these two plug-ins are shipped with the Backup Client. Click **Next** to continue.


Account Setup Wizard
Confirm your account settings.
If the settings below are correct then click Next, otherwise click Back to change your settings.
Summary
You have entered the following information:
SWISSVAULT Username: SERVER01
Connection method: Local Area Network
Automatic backups:
Backup daily at: 22H00
Help
< Back
Next >
Cancel

Step 8 of 8
Confirm that the information you supplied is correct, and click **Next**.

The Backup Client will connect to the StorageCenter and configure your account. A message will be displayed to confirm that your account was created successfully.

Click **OK** to close the message box.

Next, you must select files and folders, to create your selection list.

2.3 Security – Access to the Backup Client

The SWISSVAULT SE Service needs access to all files that must be protected. If you have folder permissions enabled on your server, you have to ensure that the service is started with a user that has sufficient rights to access these folders, e.g. started with the administrator account.

Everyone who has access to the SWISSVAULT Server Edition backup client will be able to restore files, whether they have file/folder permissions or not, so access to the server and the SE Backup Client must be controlled.

You have two options to increase the security level in Server Edition:

- Enable the setting **Prompt for password on restore** in the **Account and Security** tab by selecting **Options** from the **Tools** menu. With this setting enabled, users will not be able to restore any files without the proper account password.
- The second option is to set permissions to the SWISSVAULT SE folder, to ensure that only authorised users can access the folder. If you set permissions unauthorised users will not be able to run the Backup Client to modify the file selection or to restore files. **Note that you must still configure the SE service to start with a user that has access to the folder and to the protected files**.

2.4 Server Edition Auto-Update

As from v4.1, the Backup Client will automatically receive software upgrades during scheduled backups, should there be an update available on the StorageCenter and if Auto-Update is enabled for the particular Group in the StorageCenter Console. Nothing needs to be configured in the Backup Client.

Note: After an auto-update, you must restart the Backup Client GUI before the new version will be visible. You are advised to keep the GUI closed, when not used.

3 The Backup Service

The SWISSVAULT Server Edition (SE) service initiates automatic backups in the background at scheduled times. You do not have to be logged in for the service to backup your data, as with any Windows service.

If you are protecting files and/or folders with permissions, you have to ensure that the SE service is started with an account that has the required permissions to gain access to the files and/or folders.

3.1 Server Edition Runner

The SE Runner (the icon in the system tray) monitors activity of the backup service and can also be used to select various options for the Backup Client. An animated icon indicates that the service is busy with a backup process.

If you right-click on the SE Runner you will see the following options:

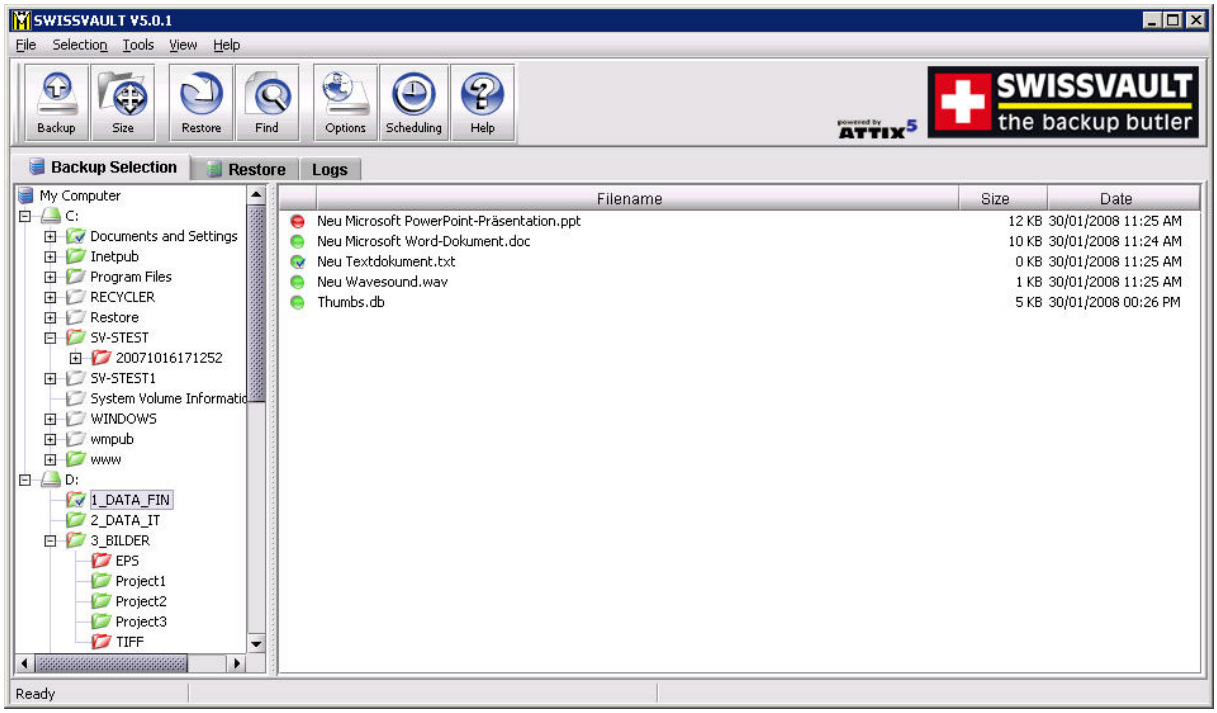
Open	To open the SWISSVAULT Client where you can modify your backup selection, restore files and configure the backup schedule. You can also double-click on the SE Runner to open the Backup Client.
Backup Now	With this option you can manually initiate the backup process without opening the Backup Client.
Cancel Backup	If the service is busy with a backup (an animated SWISSVAULT icon), you can click on cancel to stop the process.
Monitor Progress	With this option you can monitor the status and progress of the process that the SE Runner is busy with at that moment without opening the Backup Client. A small window is opened above the system tray and displays the current process and progress.
About	About displays a window with the product details. Click anywhere on the About window to close it.
Exit	If you click on Exit the SE Runner will be removed from the system tray, but it will not stop the SWISSVAULT service from running scheduled backups. If you want to see the icon in the system tray again, open the SWISSVAULT Backup Client.

When the service is busy with a backup, you will notice that the system tray icon is animated. The Backup service must be running at all times otherwise backups (manual or scheduled) will not be able to take place.

If you need to stop or start the Backup Service, open the **Services** window in the **Control Panel**, click on **SWISSVAULT SE** and select **Stop** or **Start** from the toolbar. The system tray icon is displayed with a red cross when the service is not running.

4 Backup Client

SWISSVAULT Server Edition keeps your most valued data secure. It allows you to select files and initiate backups, and to restore lost or corrupted files. You can also find and restore files from previous backups and schedule automatic backups.



While you are using the Backup Client, you may select **Help** from the **Help** menu, should you require any help. This additional windowpane on the right of the window above, will guide you through the operation of the Backup Client.

4.1 How to Backup

The next sections describe how to select files and folders for backup, how to add filters to folders to automate the file selection of certain file types, and how to backup your files to the StorageCenter.

4.1.1 Selecting Files for Backup

To select files that you would like to backup, click on the **Backup Selection** tab. The folder structure of your computer is displayed in the left-hand pane. If you click on a folder, its contents will be displayed in the right-hand pane. Subfolders are only shown in the left-hand pane. Once a file or folder is selected for backup any changes, additions or deletions to that file or folder are automatically backed up.

To select an individual file: Browse to the individual file that you would like to backup. In the right-hand pane, right-click on the file and choose **Select** or click in the box next to the file. A selected file is displayed with a green icon. To deselect a file you can either click on the box again or right-click on the file and **Deselect** it. Folders that have some files selected are displayed with a green tint.

To select an entire folder: Right-click on the folder and select **Include Folder**. You can also use the left mouse button to highlight the folder and then **Include** the folder from the **Selection** menu. Included folders are displayed with a green folder. All files in the included folder and its subfolders are now selected for backup. Any changes made within this folder or its subfolders will automatically be included as well. To deselect a folder, right-click on the folder name and select **Deselect Folder** from the selection list**.**

To exclude a file or folder: If an entire folder is included but you want to exclude a particular file or subfolder, right-click on the file or folder and select **Exclude**. Excluded items are displayed with red icons or red folders. Folders that have been selected but have some files or subfolders excluded are green with a red tint.

To verify the size of your backup, select **Calculate Size** from the **File** menu or click on the **Size** button in the toolbar. If your backup set is larger than your allocated limit you have to reduce the size of your selection. To remove files, right-click on a file that you want to exclude and click on **Deselect**. Alternatively, you can ask your backup administrator to upgrade your account limit.

Note: The Backup Client compares your backup account size with the size of your backup selection at the beginning of the backup process. The backup process will stop and an error message will be displayed if the selection size is over your account limit.

If you do not want to wait for the next automated backup, you can select **Backup Now** from the **File** menu to manually start the backup process.

4.1.2 Filters

You can use a filter to automate the file selection of particular file types from a specific folder and its subfolders. For example, a ***.doc** filter will include all existing Word documents, as well as any new Word documents that may be added later. To add a filter to a specific folder, right-click on the folder, select **filters** and choose one of the available filters from the list.

A few filters have been provided for you to start with. You can create, modify and delete any of the filters. To modify a filter, select **Filters** from the **Selection** menu and click on **Edit filters**. Select one of the filters and **Add** or **Remove** any of the file types. The **New filter** option allows you to add additional filters. Supply a name that describes the filter and then enter the file type(s).

Example: AutoCAD users may want to only select their drawing files as the rest are generated by AutoCAD and do not need to be backed up. The filter could be called Drawings and the filter type would be ***.dwg**.

Files that are included by applying a filter are displayed with the green selection icons with a blue checkbox, e.g. for files, and for folders. Filtered files or folders cannot be deselected, but you can exclude particular filtered files or folders by right-clicking on the file or folder and then selecting **Exclude**. A filtered folder with exclusions is displayed with a red tint. More than one filter can be applied to a specific folder. To remove filters from a folder, right-click on the folder, select **Filters** and clear the checkbox next to the specific filter(s) that you want to remove.

4.1.3 Profiled Selections

You may notice another group of icons in the Backup Client. Dynamic Profiling selections, which can be specified by the Backup Administrator, are displayed with the following images: for file inclusions, for filtered inclusions and for excluded files. On folder level, the images are for included folders, for filtered folders, and for excluded folders.

4.1.4 Manual Backups

After you have selected the files and folders for backup, you can manually initiate the backup process by selecting **Backup Now** from the **File** menu or by clicking on the **Backup** button in the toolbar. You may close the Backup Client after you have started the backup process by clicking **Hide**. This will not cancel the backup process and you can at any stage open the Backup Client to view the progress of the backup. You can also monitor the backup progress by right-clicking on the system tray icon and selecting **Monitor Progress**. Backup log information can be viewed in the **Logs** tab. Backup entries are displayed in blue.

Note: The backup selection list is automatically saved every 30 seconds. Right-clicking on the SE Runner and selecting Backup Now will not backup any files selected within the last 30 seconds. You have to close the Backup Client or wait a few seconds before these files will be saved.

4.1.5 Backup Resume

The Backup Client can try to resume a backup, if the previous request failed for whatever reason. If you select **Backup Now** from the **File** menu or you click on the **Backup** button in the toolbar and the previous backup was not successful, the Backup Client will prompt "**Do you want to resume the failed backup?**" with a 30 second countdown. If you select **Yes**, the Backup Client will try to continue from where the process failed during the previous backup. Select **No** to initiate a new backup or **Cancel** to return to the Backup Client.

Note: A new backup will be initiated after the countdown has elapsed.

4.1.6 Multiple Thread Backups

SWISSVAULT Server Edition supports multiple thread backups. Files are transferred to the StorageCenter using a second thread as soon as they are compressed or patched while the backup process continues to compress/patch files using the first thread in the background. This improves the total backup speed significantly.

Note: this functionality is enabled by default. To disable this feature please refer to the Advanced Options section later in the user manual.

4.2 How to Restore

The next section describes how to select the files that you want to restore, how to search for specific backed up files, and finally how to restore files from the StorageCenter.

4.2.1 How to restore files and folders

Open the **Restore** tab. From this tab, you can gain access to your backed up files. Your latest backup is shown in the **Last Backup** folder. If you expand the **Previous Backups** folder, the Backup Client will connect to the StorageCenter and retrieve a list of all previous backup dates.

Select the files and/or folders you want to restore. To select a single file, right-click on the file and click on **Select** or you can click in the box next to the file. To select an entire folder, right-click on the folder and then choose **Select folder**. Selected files are displayed with green icons. To start the restore process, select **Restore** from the **File** menu or click on the **Restore** button in the toolbar.

Note: Automatic backups are disabled during the restore process.

The Backup Client will prompt for a restore location to where the file(s) must be restored. If you select **Original location**, the files will automatically be restored to the same location from where they were backed up.

Note: If you choose this option, the restored files will overwrite any existing files with the same name in that location. You will be warned before the Backup Client overwrites any files.

If you do not want to overwrite the current copy of these files, select the **Folder** option. The default path is C:\Program Files\SWISSVAULT SE\Restore. You can also **Browse** to another folder if you want to restore the files to a different location.

Restore Options:

Recreate directory structure	By default, the folder structure is recreated in the restore folder. If you want all files to be restored to one location, uncheck the **Recreate folder structure** option. **Note: If you are restoring files from different folders with the same filename, you must recreate the folder structure or they will overwrite each other.**
Restore empty folders	You can choose whether empty folders must be recreated if the **Recreate directory structure** option is enabled.
Overwrite files	Enable this option if you do not want the Backup Client to prompt you before overwriting an existing file.
Use compression (faster over the Internet)	Tick the **Use compression** option to enable compression. With this setting enabled, the StorageCenter will compress the files before transferring them to the Backup Client. **Note: You are advised to always enable this setting if you have a slow connection to the Internet as the files are smaller with this option enabled.**
Restore file and folder permissions	Disable this option if you do not want to restore the file and folder permissions; typically used after a complete server failure to restore files before users accounts are re-created.
Do not use Temp folder (resume on file level not possible)	Enable this option to write the files directly to the specified folder without using a temporary working folder. The restore process is faster with this option, but file level resume is not possible and a complete file will be resent should there be a communications error between the StorageCenter and the Backup Client during the file transfer.

Restore log information can be viewed in the **Logs** tab. Restore entries are displayed in green.

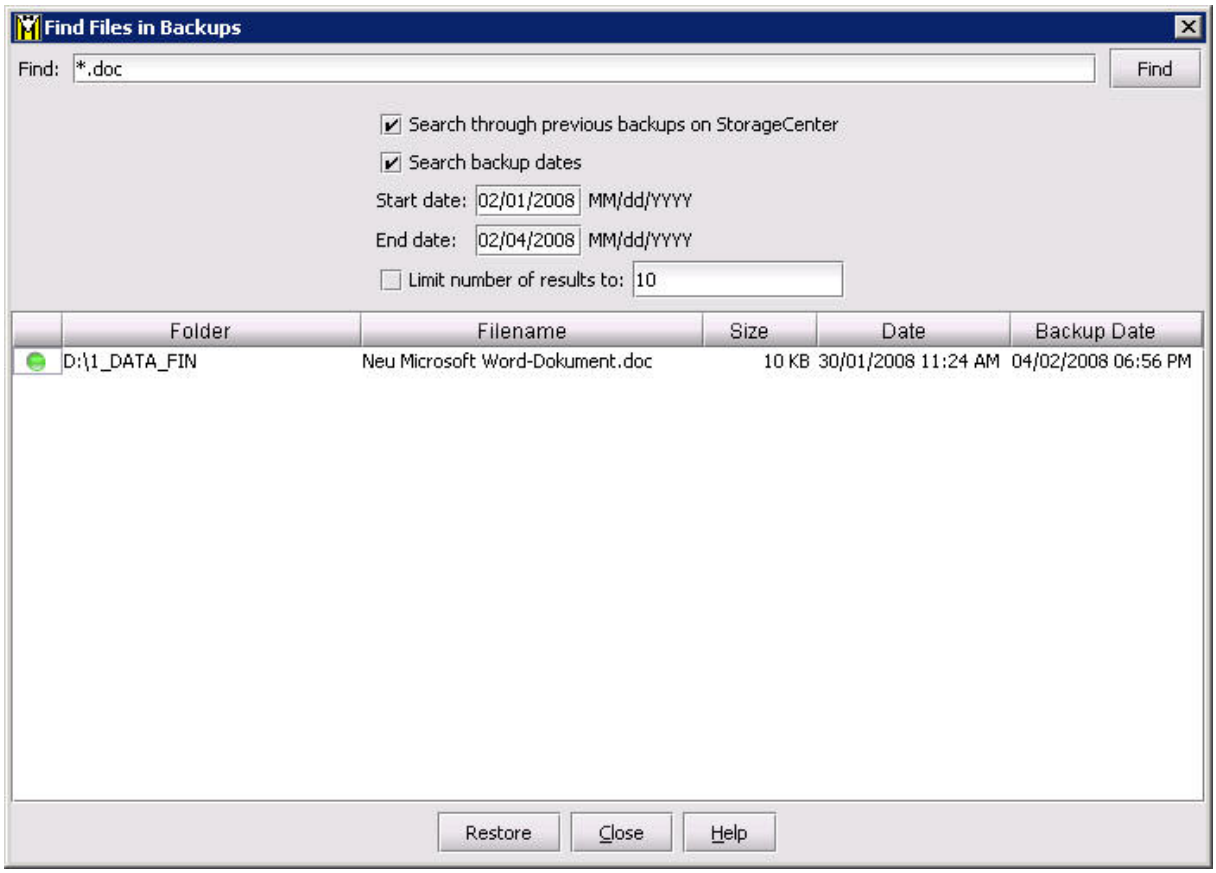
4.2.2 Finding Files

The **Find files in Backups** option enables you to search through your previous backups to find a specific file. You have the option to do a local search from your last backup, or you can connect to the StorageCenter to search through your previous backups.

To search for a file from your latest backup, select **Find files in backups** from the **File** menu or click on the **Find** button in the toolbar. Enter the filename in the textbox and click on **Find.**

Example: If you enter **help** in the textbox, the Backup Client will display a list of all backed up files from your last backup that contain help in either the filename or the folder.

Note: You can use the * and ? wildcards for advanced search queries to find the files that you are looking for.



To search for files from previous backup sets, enable the **Search through previous backups on server** checkbox.

File dates can also be specified and you can and limit the number of results that must be displayed. **Note: The Backup Date is used if you enable Search file dates and not the file create or file modified dates.**

To restore the located files, select them individually and then click on the **Restore** button.

4.3 Options and Settings

From this **Tools** menu option you can view and configure the primary Backup Client options and settings. To open this section, select **Options…** from the **Tools** menu. The various options and settings are grouped according to their functions and displayed in different tabs.

Note: Please read through this section carefully before you change any of these settings. Incorrect settings could cause serious problems or even stop the Backup Client from backing up your data.

4.3.1 Account and Security

Account Information
This section displays your backup account information as it is stored in the StorageCenter. You can use the **Retrieve Settings** button to update your account settings from the StorageCenter. This tool is useful to verify that your account limit has been modified after requesting a change from your Backup Administrator or to update Backup Group Profiling settings.

Account Setup
If you need to change your password or encryption key, select either the **Change Password** or **Change Encryption Key** buttons. Changing your encryption key involves intensive processing on the StorageCenter and may take several minutes. It should therefore not be done unless your encryption key was compromised.

Security Settings
The Security window allows you to select whether the Backup Client should remember the backup account password when running a backup or a restore. There are two options available:

- **Remember password for backup and restore**: The Backup Client remembers the user password when doing a backup or restore. This is the default setting.
- **Prompt for password on restore:** The Backup Client prompts for the user password during the restore process.
- **Prompt for password to open the backup client and to restore:** Use this option to enable access control. The Backup Account password must be supplied before you will be able to open the backup client to change the backup selection or any of the application settings. Backups will continue as normal.

4.3.2 Connections

Connection Settings
In this section, you can change the connection that the Backup Client must use to connect to the StorageCenter. You can choose between a network/permanent or dial-up connection.

The **Dial-up Settings** button is enabled if you select the Dial-up option. Click on this button to select an existing dial-up connection configured on the computer, and supply the username and password for that Internet connection.

Proxy Server
Enable the Use a proxy server for you network or dial-up connection checkbox if you connect to the Internet via a proxy server, and supply the necessary information.

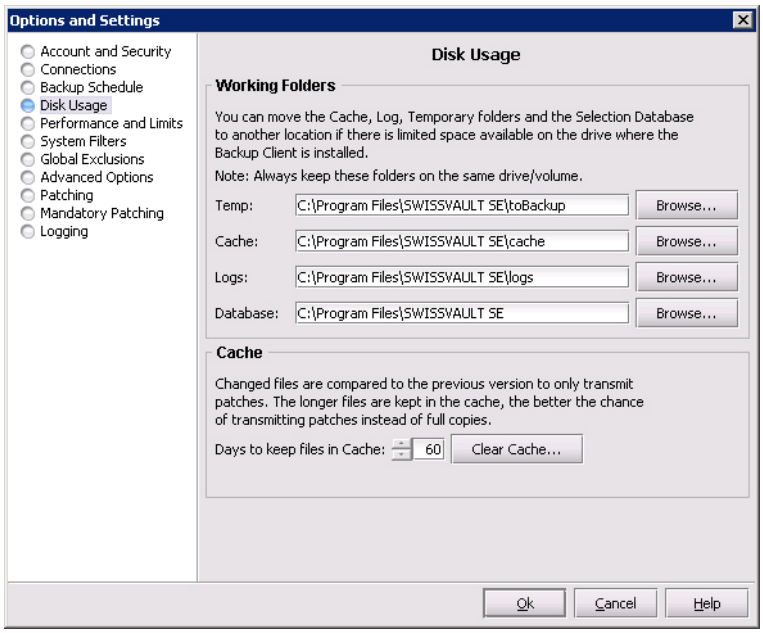
4.3.3 Backup Schedule

The Backup Client can be scheduled to backup your selected files and folders automatically. Note that if you configure the Backup Client to backup at night, the server must be powered, but you do not have to be logged in. The backup schedule can be changed by selecting **Automatic Backups** from the **Tools** menu or by clicking on the **Scheduling** button in the toolbar.

Use the **Daily Automatic Backups** section to configure a once-off daily backup. The **Advanced Schedule** can be used to specify hourly backups. Backup logs can be viewed in the **Logs** tab. Backup entries are marked in blue.

Note: You are advised not to disable automatic backups as you will then have to manually backup your files.

4.3.4 Disk Usage



Working Folders
If you have limited space on the drive where the Backup Client is installed, you can move the Cache, Logs, Temporary folders and the selection database to another location. The Temp folder is used for temporary workspace when the files are patched, compressed and encrypted, the Logs folder stores all backup and restore logs, and the Cache folder keeps a local, compressed and encrypted, copy of the selected files for a specified amount of days. The selection database compares the latest backup selection with the previous backup to determine the changes.

Note: Always keep these folders and the selection database on the same drive. If you move these folders and the database to a network share, please ensure that the Backup Client has the correct permissions to reconnect to that share.

Cache
When modifications are made to a file, the Backup Client only transmits the changes to that file, as opposed to transmitting the complete file again. This is accomplished by keeping a compressed copy of the file in a local cache and then using a sophisticated patching technique to extract the difference between the file in the cache and the one ready to be backed up.

Files are only kept in the cache for a certain amount of days. Files are added to the Cache folder if the file was modified within the **Days to keep files in Cache** window. Once a file has been flushed from the cache, a full copy must be backed up when any modifications are made to the file. The longer files are kept in the cache, the better the chance of only transmitting patches instead of full copies and thus reducing the amount of data that needs to be transmitted. If you have limited disk space, you may want to consider shortening the time files are kept in the cache.

Note: If you select 0 days, patching is disabled, any files in the Cache folder will be deleted, and complete files are backed up to the server during each backup.

To delete the current cache, use the **Clear Cache…** button. If you delete the cache, full copies of your selected files will be re-sent to the server during the next backup. You may notice that the Backup

Client will log the message **Doing monthly cache cleanup** once a month. This maintenance task is to ensure that the cache folder is up to date by deleting any files that fall outside the **Days to keep files in Cache** window.

4.3.5 Performance and Limits

Processor Usage and Disk Access

The Backup Client uses a fair portion of the available processor power to patch, compress and encrypt files while during the backup process. If you use the computer at the same time, you may experience some performance deterioration. You can lessen this effect by lowering the **Processor Usage**.

Disk Access is another setting that you can modify to limit performance deterioration. If this setting is set to high, the Backup Client will continuously use all available disk access to write to the disk, ensuring that the process completes as fast as possible. The process will take longer if you lower this setting but your other applications will still function without any interruptions.

Limits

Outgoing transfer limit - The outgoing transfer bandwidth can be limited (in kBytes/second) in case you need to allocate only a certain amount of bandwidth to the Backup Client.

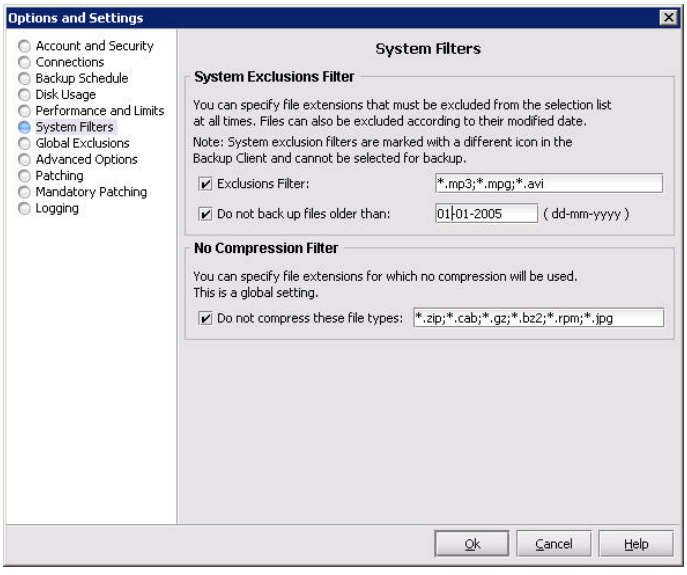
Backup size restriction - You can limit the total amount of data that may be transferred during each backup. Note: If you enable this option, it may take several backups before all your files are backed up to the StorageCenter. This feature is especially useful if you have a poor Internet connection and you encounter problems with transferring large backups.

Backup cycle - The Backup Client can be configured to cycle the backup process until all selected data has been transferred to the StorageCenter by automatically initiating subsequent backups. This setting can only be enabled if a **backup size restriction** has been specified.

4.3.6 System Filters

System Exclusion Filter

The System Exclusions Filter enables you to specify any file types that you want to exclude from the backup selection list. For example, to exclude all MP3 and AVI files, specify ***.mp3;*.avi** in the text box. Separate entries with a semicolon.


Options and Settings
Account and Security
Connections
Backup Schedule
Disk Usage
Performance and Limits
System Filters
Global Exclusions
Advanced Options
Patching
Mandatory Patching
Logging
System Filters
System Exclusions Filter
You can specify file extensions that must be excluded from the selection list at all times. Files can also be excluded according to their modified date.
Note: System exclusion filters are marked with a different icon in the Backup Client and cannot be selected for backup.
Exclusions Filter:
.mp3;.mpg;*.avi
Do not back up files older than:
01-01-2005
(dd-mm-yyyy)
No Compression Filter
You can specify file extensions for which no compression will be used.
This is a global setting.
Do not compress these file types:
.zip;.cab;*.gz;*.bz2;*.rpm;*.jpg
Ok
Cancel
Help

You can also exclude files by enabling the **Do not back up files older than:** checkbox and specifying a date. Note that the Date Exclusions Filter uses the file modify date as reference and not the file create date.

No Compression Filter

Compression is not effective on all file types as some files may already be compressed or cannot be compressed at all. The Backup Client could spend some time and processing usage to try and compress these files. This filter enables you to specify a list of file extensions that must not be compressed during the backup process. The list of file types already specified are types known for not compressing well.

4.3.7 Global Exclusions

SWISSVAULT enables you to specify File and Folder Exclusions. These files and folders are excluded from the backup selection, no matter where they are located on the available drives or volumes. **Note: these entries are case sensitive; you have to ensure that you specify exact matches**.

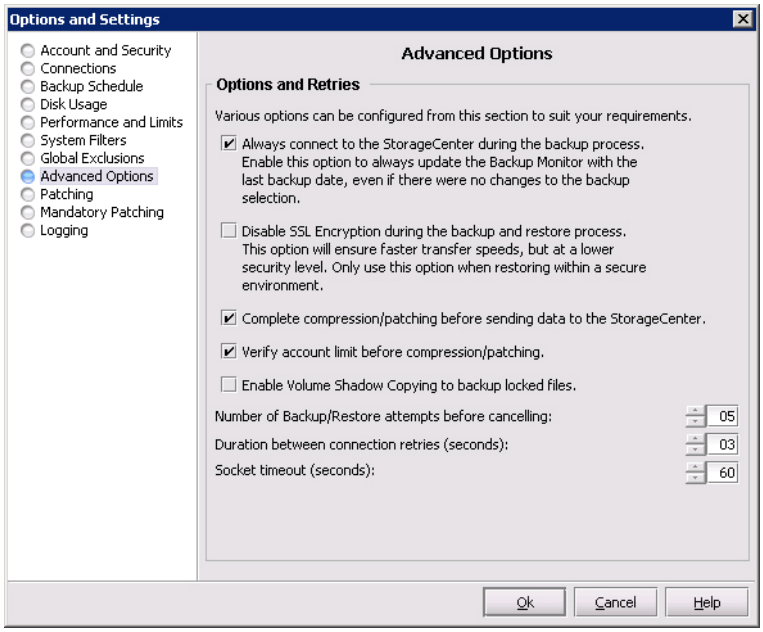
To add an exclusion, click on **Add folder** or **Add file**, specify the name and click **OK**. Folders are displayed with and files with . To modify any of the exclusions, select the entry and click on **Edit**, or double click on the exclusion name. To remove an entry, select the file and click **Remove**.

Click on **OK** at the bottom of the Exclusions tab to save your changes. Excluded files are displayed with and folders with in the Backup Client.

4.3.8 Advanced Options

Options and Retries
The Backup Client can be configured to **Always connect to the StorageCenter** during each backup to update its last backup date stamp, even if there were no changes made to the backup set. With this setting enabled, the StorageCenter will always be up to date with the latest backup date.

SSL Encryption can be disabled to improve the transfer time during the backup and restore processes. **Note: By disabling SSL encryption, you are lowering the security level when transferring files to and from the StorageCenter. This setting should only be used in a secure environment.**


Options and Settings
Account and Security
Connections
Backup Schedule
Disk Usage
Performance and Limits
System Filters
Global Exclusions
Advanced Options
Patching
Mandatory Patching
Logging
Advanced Options
Options and Retries
Various options can be configured from this section to suit your requirements.
Always connect to the StorageCenter during the backup process. Enable this option to always update the Backup Monitor with the last backup date, even if there were no changes to the backup selection.
Disable SSL Encryption during the backup and restore process. This option will ensure faster transfer speeds, but at a lower security level. Only use this option when restoring within a secure environment.
Complete compression/patching before sending data to the StorageCenter.
Verify account limit before compression/patching.
Enable Volume Shadow Copying to backup locked files.
Number of Backup/Restore attempts before cancelling: 05
Duration between connection retries (seconds): 03
Socket timeout (seconds): 60
Ok
Cancel
Help

Complete compression/patching before sending data to the StorageCenter. Enable this option if you do not want to make use of multiple thread backups to speed up the backup process, typically needed when using a dial-up account. With this setting enabled, the Backup Client will compress all new files and patch all modified files before starting to transmit data to the StorageCenter.

Verify account limit before compression/patching. With this setting enabled, the Backup Client verifies the backup account limit on the StorageCenter before starting with the compression and/or patching processes. It is useful to flag account limit issues before starting with these processes.

Enable Volume Shadow Copying to backup locked files enables you to backup locked files without using third party open file management software. This is currently only available on Windows XP, Windows 2003 Server and Windows Vista Operating Systems.

Number of Backup/Restore attempts before cancelling - By default, the Backup Client tries to connect to the StorageCenter four times before cancelling the backup process. If you have a poor connection to the Internet, you may want to consider increasing the number of attempts. The backup will continue from the previous point of failure. It will not resend the entire backup.

Connection Retries - By default, the Backup Client will try to reconnect to the StorageCenter after 60 seconds, should the connection be dropped. This setting enables you to increase/ decrease the duration between the retries.

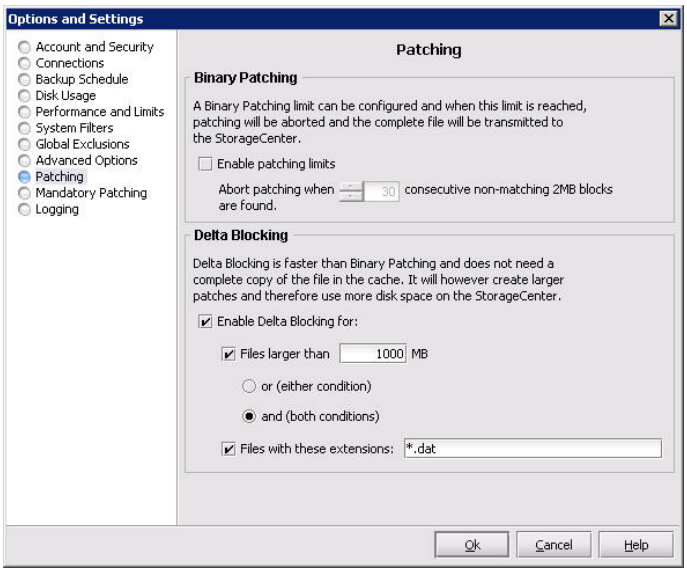
Socket Timeout - The socket timeout is, by default, 60 seconds. If the Backup Client is connected to the StorageCenter and there is no communications between the two, this amount (in seconds) is the duration that the Backup Client will stay connected before dropping the connection.

4.3.9 Patching

Patching is the process by which only the differences in files are extracted to minimize the amount of data that has to be transferred to the StorageCenter. There are two types of patching available, binary patching (the default) and delta blocking.

Binary Patching

Binary patching is the most effective form of patching. It is very CPU intensive but will deliver the smallest patches. The process is only possible if a complete copy of an older version of the file is available in the cache. Furthermore the patch must be applied to the file in the local cache which will require additional processing. Note that old copies are periodically flushed from the cache – refer to the **Disk Usage** section for more information.


Options and Settings
Account and Security
Connections
Backup Schedule
Disk Usage
Performance and Limits
System Filters
Global Exclusions
Advanced Options
Patching
Mandatory Patching
Logging
Patching
Binary Patching
A Binary Patching limit can be configured and when this limit is reached, patching will be aborted and the complete file will be transmitted to the StorageCenter.
Enable patching limits
Abort patching when 30 consecutive non-matching 2MB blocks are found.
Delta Blocking
Delta Blocking is faster than Binary Patching and does not need a complete copy of the file in the cache. It will however create larger patches and therefore use more disk space on the StorageCenter.
Enable Delta Blocking for:
Files larger than 1000 MB
or (either condition)
and (both conditions)
Files with these extensions: *.dat
Ok
Cancel
Help

Binary Patching is enabled by default and nothing needs to be configured in this tab for normal use.

Enable patching limits: It is possible that a file is modified in such a way that it becomes unfeasible to patch it. An example would be a database that is re-indexed.

In such a case the patching can take extremely long (it may exceed your backup time window) and will eventually create a patch that is the same size as the complete file. It is better to abort the patching and rather just compress the new file, and transfer it to the StorageCenter. The patching limit allows you to specify when the backup client will decide to rather abort the patch and send a full copy of the file.

To specify patching limits, enable the checkbox next to **Enable patching limits** and specify the amount of consecutive blocks. When this amount is reached, patching will be aborted and the complete file will be compressed and resent to the StorageCenter. **Patching Limits should only be enabled if you have serious patching issues with large files.**

Delta Blocking

An alternative solution to determine the change between two versions of a file is Delta Blocking.

Note: It is vital that you read through this section before enabling this option in your Backup Client.

The Delta Blocking process is significantly faster than Binary Patching and it does not require a complete copy of a file in the cache to calculate the patch, only a footprint file. The footprint files require very little free disk space, as a single footprint file is only 0,0006% of the original file.

The patches are, however, much bigger than Binary patches so Delta Blocking should only be used if you backup to a local StorageCenter or if you have a very good Internet connection. The StorageCenter also requires additional free hard disk space because of the larger patches. Delta blocking patches are created by comparing “blocks” of data for any change since the last backup.

Enable the checkbox next to **Enable Delta Blocking**. You can set the Delta Blocking file selection criteria in two ways, either by file size or by file type. Select the applicable condition(s) and supply the necessary information. Both conditions can also be enabled by selecting both conditions and the “**and**” option. Any recently changed files not matching these criteria will be patched using binary patching.

Note: Some database files may not be suitable for binary patching since data is shifted at the beginning of the file. When this happens it will result in a patch as large as the complete file. It is advisable to closely monitor the sizes of the patches when Delta Blocking is enabled and rather disable it if it turns out to be ineffective.

4.3.10 Mandatory Patching

Mandatory files are scanned for changes, regardless of whether it appears that they have changed since the last backup. This is useful in situations where files are held open by an application – internally the file changed, but the change is not reflected in the last modified date on the file system, or in the size of the file itself.

Open File Manager/VSS enables the backup of these files without impacting the running application or corrupting the indicated file.

4.3.11 Logging

The **Logs** tab in the backup client provides detailed information about each backup and restore. This section enables you to modify the structure of these log files. You will notice an additional toolbar button when you open the Logs tab; the Summary button can filter the information to only display the last 14 lines.

Log File Content

You can specify the level of information that must be included in the log files. Choose between:

- Log all messages
- Suppress detail messages
- Only log errors and warnings

Enable the **Include date in log file time stamp** checkbox to add the date to the backup and restore log files.

Automatic Log File Deletion

A log file retention period can be enabled to delete files older than e.g. 30 days by enabling the checkbox and specifying the duration in days.

4.4 Additional Settings

The **Tools** menu provides you with various options and settings that you can modify to enhance and streamline your Backup Client. You can also modify your account settings from this menu.

4.4.1 Add Network Volume

You have the option to add network volumes and include files located in these locations to your backup selection.

Note: You have to ensure that the backup service is started up as a user that has sufficient permissions to browse and access the network shares.

The Backup Client will only be able to backup files from a network volume after the share has been accessed and authenticated by the server where the Backup Client is installed.

To add a network volume, select **Add Network Volume** from the **Tools** menu. Enter the UNC network path in the space provided. Paths must to start with "****" before they will be accepted, for example \\File-Server\documents. You can also use the **Browse** button to browse to the network path. Network volumes are listed in the left-hand pane after they have been added and displayed with a network image. If some files are included the image will change to and if you include the entire share it will change to a green image. Excluded network volumes are marked with red network images.

Without the correct permissions the Backup Client may still be able to display the files on the share, but it will not be able to access these files during the backup process. You will see a message **Volume \\File-Server\documents\ is not available for backup** in the log file if the Backup Client cannot access these files.

You can remove a network volume from the Backup Client by right-clicking on the entry in the left-hand pane and then selecting **Remove Network Volume**.

4.4.2 Remote Management

Remote Management enables you to remotely access and configure the Backup Client from the StorageCenter Console.

To enable this feature, select **Remote Management** from the **Tools** menu and enable the checkbox next to **Enable Remote Management**. The **Allow SC controlled access** option enables backup administrators with the correct access permissions to use their StorageCenter User Access Management username and password to connect to and administer this Backup Client. If you disable this checkbox, StorageCenter administrators will not have remote access.

Specify the port number (the default port is 9091) that must be used for Remote Management. If the server has multiple IP addresses available, you can specify whether the Remote Service must bind to **All** or **Only** to one IP by specifying the address in the textbox.

Enable the **Allow custom access** option and supply a username and password if you do not want to make use of the above-mentioned StorageCenter Access Accounts. This custom access username and password must be specified in the StorageCenter Console to gain remote access. Click **OK** to save you settings. After the service has been restarted, click on **OK** to close the window.

4.4.3 Health Check

The Backup Client Health Check provides information to pre-emptively highlight possible issues, for example free disk space problems or SE service access rights to files and folders. It can also provide the estimated line speed to the StorageCenter. Five sections are available:

- **Memory** – Memory utilisation statistics from the last backup as well as overall memory usage to date.
- **Data Protected** – Information includes the number of files and directories selected for backup.
- **Disk Usage** – Free space availability for all local drives.
- **Line Speed** – Line Speed estimate to the File-Server by transmitting data for 10 seconds.
- **Service Rights** – Information about the service account name and access rights to the working folders.

You can decide which checks you want to run by enabling/disabling the checkboxes next to the entries. Use the **Show Last Health Check** button to see the last report. You have the option either **Print** or **Export** the Health Check reports.

4.4.4 Volume Shadow Copy Service

Applications often keep their data files locked if the application is running. This is usually a problem when trying to backup these files as the application does not allow the backup agent access to the file to determine the changes since the last backup.

Microsoft Volume Shadow Copy Service (VSS) provides a solution by automatically creating a snapshot of the data at any given point in time without any interruption to the application, and without the need for any third party software.

VSS is currently available on Windows XP, Windows 2003 Server and Windows Vista operating systems and enabled by default in Server Edition. If you are using the current Open File Manager plug-in, and you would like to continue using the plug-in, you have to disable VSS in the Backup Client as the two processes cannot run simultaneously. Select **Options…** from the **Tools** menu and then the **Advanced Options** tab. Disable VSS by removing the check in the checkbox next to **Enable Volume Shadow Copying to backup locked files**.

Note: You must continue to use the available SWISSVAULT plug-ins to protect your mail servers or databases at this stage as SWISSVAULT VSS support is currently limited to locked files.

4.4.5 Snapshot Backup and Restore

Snapshot Backup and Restore enables you to create a backup of your selected files on a local Snapshot server within your Local Area Network (LAN). This Snapshot server will then be physically moved to the server running the StorageCenter where the data will be transferred.

The StorageCenter is hosted on the SWISSFORTKNOX Data Centre and this feature enables the backup administrator to reduce the initial backup window if there is a large amount of data that must be backed up, typically across a slow internet/network connection. A similar procedure can be followed when restoring a large amount of data, for example, during a Disaster Recovery.

Snapshot Backups

Note: Only the backup administrator should configure or change these settings.
Two options are available in the Backup Client, **Snapshot to disk** and **Snapshot to Snapshot server**. Using the second option, you must add a Snapshot server to your LAN, initiate the backup, and then connect the Snapshot server to the StorageCenter and transfer the data with the Snapshot Tool. With the Snapshot to disk option, you do not need any additional software; simply create the Snapshot backup on disk and then transfer the data to the StorageCenter using e.g. an external drive.

Snapshot to Disk

Open the Backup Client and select the files that must be backed up. Select **Snapshot** from the **Tools** menu, and click on **Backup**. Enable the checkbox next to **The next backup must be a Snapshot backup**. **Send Snapshot to disk** is selected by default. Specify the location where you would like to create the Snapshot backup. Enable the checkbox next to **Update index from StorageCenter before Snapshot** if you want to update the index file before initiating the Snapshot process, typically if there are already previous backups available on the StorageCenter for this particular account.

Initiate a backup by clicking on the **Backup** button in the toolbar or **Backup Now** from the **File** menu. The backup account is automatically disabled after a Snapshot backup to ensure that the data can be moved to the StorageCenter before the next backup is initiated.

Your backup administrator will move the local snapshot folder to the StorageCenter and your account will be enabled again.

Snapshot to a Snapshot server

A few steps are necessary to ensure that everything is in place to backup to the Snapshot server:

- Connect the Snapshot server to the LAN where the Backup Client is located.
- Ping the Snapshot server from the Backup Client computer to establish whether you can communicate with the Snapshot server. Make a note of the IP address/Hostname.

The following settings must be configured in the Backup Client. Create an account for the specific Backup Client but **do not backup any files to the account**.

- In the Backup Client select **Snapshot** from the **Tools** menu and click on **Backup**. In the **Snapshot backup** settings window, supply the Snapshot backup server address as well as the server port. The default port is 8443. Click in the checkbox next to **Do next backup to snapshot backup server** to enable the Backup Client to send the next backup to the Snapshot server and not to the actual StorageCenter. If the Backup Client is configured to connect through a Proxy server, you will be able to check/uncheck the “Use proxy settings for snapshot backup”. If this option is checked, the Proxy server will be used for communications to the FileServer. If it is unchecked, the Proxy server will only be used for communications to the NameServer. Click on **Ok** to accept these settings.
- Select all the files that must be backed up and select **Backup Now** from the **File** menu. These files will be compressed and backed up to the Snapshot server. Note that the user account will be disabled after a snapshot backup. This is to ensure that the user will not initiate another backup before the data has been transferred to the StorageCenter.

Snapshot Restores

After the required folders have been moved to the Snapshot/DR server by the backup administrator, move the Snapshot/DR server to the LAN where the Backup Client is located.

Ensure that you can ping the server from another computer on the network. Make a note of the IP address/Hostname. The following settings must be configured in the Backup Client.

- Open the Backup Client. Select **Snapshot** from the **Tools** menu and click on **Recover**. In the **Recovery settings** window, supply the DR server address as well as the server port. Port 8443 is the default port. Click in the checkbox next to **Do restores from recovery server** to enable the Backup Client to restore from the DR server and not to the actual StorageCenter. Click on **Ok** to accept these settings.
- Open the **Restore** tab and select Previous Backups. The Backup Client will connect to the DR box and retrieve a list of all the available backup dates. From here the user will be able to restore large amounts of data. Remember to remove the tick mark in the checkbox after the restore.

4.4.6 Archive References

Archive References enables you to view backups that have been archived to another storage device, e.g. to tape. These files are marked with a greyed-out folder in the Restore tab. You can search through the available archived backups, but they cannot be restored from the Backup Client. After you have found the files that you want to restore, contact your backup administrator and request that the archived backup is moved back to the StorageCenter. Thereafter you will be able to restore the files.

These archives are only available if it has been enabled by the Backup Administrator.

4.4.7 Command Line Backup and Restore

You can use the command line interface to remotely run the Setup Wizard, enable SE Remote Management and to send a wide range of backup and restore commands to any Server Edition backup client in your organisation.

The CLI.bat file is included with each Server Edition installation file. **Note that the SE Backup Client is required and must be installed on the computer from where you want to use the CLI.bat file.**

Remote Management must be enabled in the Backup Client and a username and password set for any commands to work. Run cli -configure {account|remote} to run the Setup Wizard or to enable Remote Management in the Backup Client. You can also specify the host address with the –h command. See examples below.

Usage:

```
cli -u user -p password {restore|dates|status|backup|cancel}
[-h host] [-pt port] [-rd restoredateidx] [-rp restorepath | -original]
[-fd filterdate] [-fp filterpath] [-fext filterext]
[-compression on|off] [-overwrite]
```

Note:

- `-rp <restorepath>` must be an absolute path and the service must have full access rights to the directory.
- When restoring, the default policy is to skip existing files. Specify `-overwrite` to overwrite existing files.

Examples:

To start a backup on the local machine using the default port

```
cli -u admin -p pass backup
```

To see the status of a currently running task in the backup service

```
cli -u admin -p pass status
```

To see a list of available backup dates to restore from

```
cli -u admin -p pass dates
```

To start a restore from the last backup made, extracting files to the default restore temporary directory

```
cli -u admin -p pass restore
```

To restore from a different date, use the dates command to get a date index

```
cli -u admin -p pass -rd 2 restore
```

To restore all .XLS files starting with the path C:\Documents and Settings and newer than 1 April 2002

```
cli -u admin -p pass -fd 04/01/2002 -fext .XLS -fp "C:\Documents and Settings"
restore
```

To cancel the current running task on a remote backup service running on 192.168.20.99

```
cli -u admin -p pass -h 192.168.20.99 cancel
```

4.4.8 Dynamic Profiling

Dynamic Profiling enables your Backup Administrator to propagate certain client side settings from the StorageCenter to your Backup Client. **Note: These settings take priority over any settings specified in the Backup Client.** They include:

- Changing the backup schedule
- Specifying file and folder selections and exclusions
- Adding additional filters to the filter list
- Most **Options and Settings** found in the **Tools** menu

When the Backup Client connects to the StorageCenter, it will receive a list of any Dynamic Profiling settings specified by the Backup Administrator and these changes will be implemented in the Backup Client.

You can manually connect to the StorageCenter by clicking on the **Retrieve Settings** button in the **Account and Security** Options section, to update Dynamic Profiling settings. Profiled settings are greyed out, and cannot be modified from within the Backup Client.

4.4.9 Language

If multiple languages are available, the Backup Client will select and display the default OS language. You have the option to change this setting. From the **View** Menu, go to **Languages** and select one of the available options.

4.4.10 Look & Feel

You have the option to change the look and feel of the Backup Client. From the **View** Menu, go to **Look & Feel** and select one of the available options.

4.4.11 Advanced Settings in properties files

Please note that this section should only be used if you are familiar with the SWISSVAULT Server Edition software. **These settings can cause your backup client to stop working if not configured correctly.**

Server Edition default port
The Server Edition default port is used to communicate via TCP/IP. It is possible that a different application also uses the same port. This problem occurs when a **Veritas Backup Product** is used at the same time on the Server.

In this case, the default port has to be changed. To change the SE service default port, stop the **SWISSVAULT SE** service in the services window from the Control Panel. Browse to the folder where Server Edition is installed (the default folder is C:\Program Files\SWISSVAULT SE\) and open the a5backup.properties file. Add the entry **service.port=10001** and replace 10001 with the port number that you want to use. Start the **SWISSVAULT SE** service again, open Server Edition and confirm that you can initiate a backup and transfer data to the StorageCenter.

5 Plug-ins

Adding to its features and functionality, SWISSVAULT Server Edition also provides a solution for numerous databases and applications. These solutions are provided as plug-ins to the SWISSVAULT Server Edition software.

This user manual includes instructions for the Email notification and system state plug-ins, as they are distributed with the Server Edition Backup Client. Please refer to the **SWISSVAULT Server Edition Plug-ins** user manual for detailed information about the available plug-ins and settings.

Plug-ins currently available:

- MS Exchange 2000 / 2003 / 2007
- MS SQL 7 / 2000 / 2005
- MS SharePoint 2003
- MS VSS Database plug-in for supported databases and applications
- Sybase ASE12.5
- Lotus Domino 5 / 6.5 / 7
- Oracle 8i / 9i / 10g
- Single Mailbox Recovery for Exchange 2000 / 2003
- Email Notification (included)
- System State Plug-in (included)
- Script Plug-in

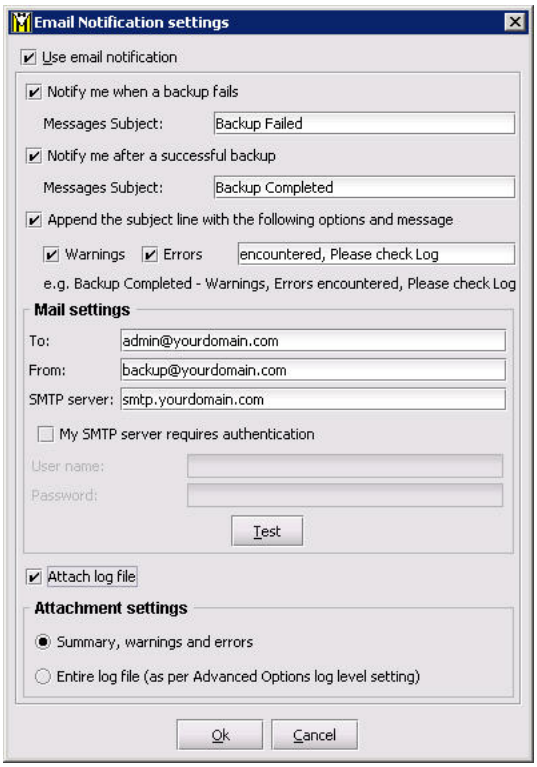
5.1 Email Notification

The Email Notification plug-in enables you to receive email notification on backup activity. You can configure the plug-in to notify you on a specified email address when a backup has been successful, when it failed or both.

5.1.1 Installing the Email Notification Plug-in

This plug-in is included in the Server Edition installer as of v5.0. If it is not installed, run the Plug-in Installer and select the **Email Notification** plug-in. After the installation, open the Backup Client interface.

5.1.2 Configure and Use



To configure the Report plug-in, open the **Tools** menu, select **Plug-ins** and click on **Email Notification**. Enable the checkbox next to **Use Email notification** to enable the plug-in. Select whether you would like to receive notification for successful and/or failed backups. You can modify the email subject. Note that the account name is automatically included in the subject, e.g. Backup Completed [User One].

If **Notify me after a successful backup** is enabled, you can choose whether Warnings and/or Errors must be highlighted in the email subject by enabling the checkbox next to **Append the subject line with the following options and message**. An example of the message is displayed below the text box.

Supply the **To** and **From** email addresses and the **SMTP server** address and authentication settings if needed.

You can specify whether the backup log must be included in the email. Choose between the **Summary, warnings and errors** or the **Entire log file**, as specified in the **Advance Options** Log level setting.

Click on **Test** to verify that the settings are correct. A message will confirm if the email was sent successfully. Click on **OK** to remove the message and **OK** again to close the Notification settings window.

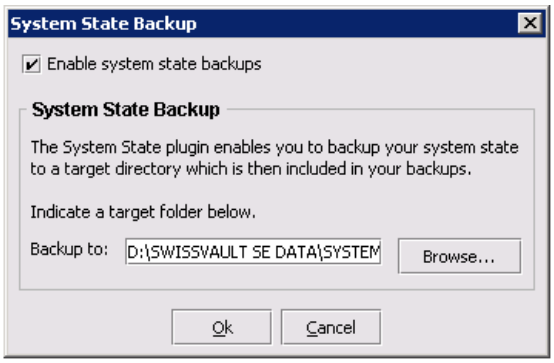
The Email Notification plug-in is now activated and will start emailing reports during the next backup.

5.2 System State Plug-in

The SWISSVAULT System State Backup plug-in enables you to backup your System State to a target directory that is automatically included in your daily backup routine. Please note that this plug-in is only available from MS Windows 2000.

5.2.1 Installation and Configuration

This plug-in is included in the Server Edition installer as of v4.2. If it is not installed, run the SWISSVAULT SE Plug-in Installer and select the **System State Backup** plug-in. After the installation, open the Backup Client interface.


System State Backup
Enable system state backups
System State Backup
The System State plugin enables you to backup your system state to a target directory which is then included in your backups.
Indicate a target folder below.
Backup to:
D:\SWISSVAULT SE DATA\SYSTEM
Browse...
Ok
Cancel

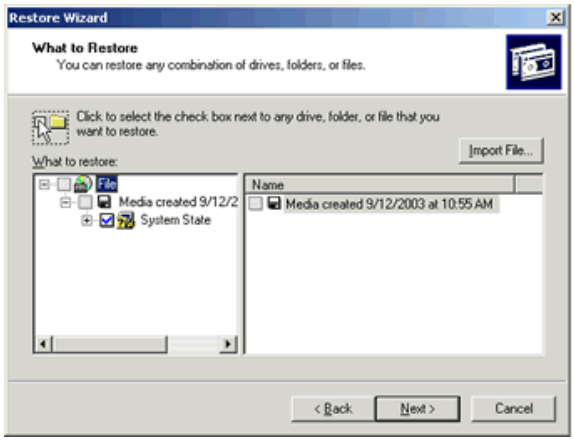
From the **Tools** menu, select **Plug-ins** and then **System State**.

Click in the checkbox next to **Enable System State** backups to enable the plug-in. A local target folder is required to create the System State backup. Please supply or **Browse** to the target folder and click **OK**. If the target folder does not exist, the Backup Client will prompt whether the folder must be created. This folder is automatically included in you backup selection list.

The System State Backup plug-in is initiated at the beginning of each backup. It uses the Windows Backup and Recovery tools to create the backup file. Server Edition continues with the rest of the backup procedure after the System State Backup has been saved in the specified target folder.

5.2.2 Restore Process

Open the **Restore** tab in your SWISSVAULT SE Client. Select the backup date that you want to restore from in the left-hand pane and restore the sysstate.bkf file that is located in the target folder.


Restore Wizard
What to Restore
You can restore any combination of drives, folders, or files.
Click to select the check box next to any drive, folder, or file that you want to restore.
Import File...
What to restore:
File
Media created 9/12/2
System State
Name
Media created 9/12/2003 at 10:55 AM
< Back
Next >
Cancel

Open the Windows Backup and Recovery application (Start >> Programs >> Accessories >> System Tools >> **Backup**) and select the **Restore Wizard** from the **Tools** menu. Click on **Import File** and browse to the restored sysstate.bkf file. The default restore location is C:\Program Files\SWISSVAULT SE\Restore.

Click **OK** to import the file. In the left-hand pane, expand Media Created and select System State. Click **Next** and **Finish** to compete the Restore Wizard.

6 Security

SWISSVAULT uses a combination of Blowfish encryption and SSL secure data transmission to ensure the safety of your data.

When the Backup Client has to transfer data to the StorageCenter, it connects using a secure SSL (2048 bit RSA key exchange, 128 bit RC4 stream cipher and SHA-1 integrity checking) connection to transfer the data. Signed SSL certificates and Certificate Revocation Lists (CRLs) are used to verify server integrity.

Data is stored using 448-bit Blowfish encryption to encode the data on the Server. This is considerably greater than the encryption used for Internet banking and online credit card transactions.

The SWISSVAULT StorageCenter uses your encryption key to generate a 448-bit primary key (55 characters). For the effective encryption of your date the primary key will be used. Your defined encryption key will NOT be stored on the StorageCenter and cannot be reset by SWISSVAULT.

The primary key is safely encrypted on the StorageCenter through your encryption key. Without the encryption key you cannot encode the primary key for backups and restores. If you change your encryption key, you do not have to remember the previous encryption keys for future restores – the Backup Client will be able to retrieve the data from the StorageCenter.

Note: If you forget this encryption key, it will render your data unrecoverable.

Blowfish Encryption

Blowfish is an encryption algorithm. It is a symmetric block cipher, which uses a variable-length key from 32 bits to 448 bits. SWISSVAULT uses the maximum strength 448-bit key.

SSL Communication

The Secure Sockets Layer (SSL) is a commonly used protocol for managing the security of data transmission. SWISSVAULT makes use of the SSL protocol (2048 bit RSA key exchange, 128 bit RC4 stream cipher and SHA-1 integrity checking) for secure communication between the Backup Clients and the StorageCenter, including data transmission.

7 SWISSVAULT Support

Please do not hesitate to contact us in case of any questions.

Note: You ideally reach us by email support@swissvault.ch, where we will reply instantly.

SWISSVAULT AG
Haldenstrasse 5
CH-6340 Baar
Switzerland

Email: support@swissvault.ch
Hotline: +41 (0)900 782 858 (CHF 2.— from the 3rd minute)
Fax: +41 (0)41 726 03 27
Homepage: www.swissvault.ch